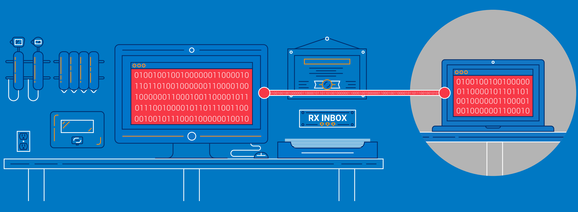
HOW HIDDEN ENCRYPTED THREATS IMPACT HEALTHCARE ORGANIZATIONS TODAY



Healthcare organizations are being increasingly targeted by cyber criminals seeking to steal electronic protected health information (ePHI), electronic health records (EMR), personally identifiable information (PII) and other confidential patient data. As the Internet moves toward 100 percent encryption to protect sensitive data, new threat vectors continue to emerge as attackers hide their activities behind SSL with increasing frequency. What dangers are pushing past your security infrastructure?

Discover the challenges you and your healthcare peers now face — including threats hiding in SSL traffic.

ARE HEALTHCARE ORGANIZATIONS EXPOSED TO CYBER THREATS?

56%
of healthcare organizations say that **less than half** of their Web traffic is inspected for attacks

81%
of healthcare organizations say they have definitely or likely been victim to a **cyber attack** or malicious insider activity in the past year

Of those,

61%
either **didn't attempt encryption** to evade the attack—or aren't even sure if they did

68%
of healthcare organizations agree or strongly agree that their infrastructure's inability to inspect encrypted traffic is a **barrier to compliance** now and in the future

ENCRYPTION IS INCREASING, BUT HEALTHCARE ORGANIZATIONS NEED DECRYPTION

Nearly **50%**
of healthcare organizations think network attackers will **increase encryption use** in the next year

55%
of healthcare organizations **don't decrypt** web traffic to detect intrusions

55%
of healthcare organizations **don't think** they'll implement decryption in the next year

47%
of healthcare organizations agree or strongly agree that SSL traffic that is malicious could cause a **costly data breach**

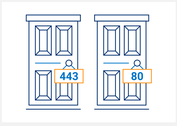
But only
18%
strongly agree that their company is equipped to detect malicious SSL traffic

DESPITE ALL THIS,

1 in 3 say SSL is essential to their company's overall security infrastructure

HEALTHCARE ORGANIZATIONS EXPECT ENCRYPTED THREATS BUT THEY AREN'T PREPARED*

Attackers use encryption to hide data exfiltration over standard ports, like 443 or 80



68% say this is extremely likely to happen

12% say they are properly equipped to resolve it

Attackers use SSL to make phishing sites look more legitimate and hide malware from IPS

57% say this is extremely likely to happen

8% say they are properly equipped to resolve it

Attackers use SSL to disguise communications with external sites

46% say this is extremely likely to happen

8% say they are properly equipped to resolve it

*In this case, "extremely likely" and "extremely equipped" are each defined by respondent ratings of 9-10 on a scale of up to 10.

TOP REASONS SSL HASN'T BEEN IMPLEMENTED BY HEALTHCARE ORGANIZATIONS

59%
Lack of performance

44%
Lack of right tools

34%
Lack of in-house expertise

SSL DECRYPTION TOOLS: MUST-HAVES

85%
of healthcare organizations agree that **scaling** to meet current and future SSL performance demands is important, very important or essential

81%
of healthcare organizations agree that **maximizing** uptime, performance requirements and security infrastructure capacity is important, very important or essential

48%
of healthcare organizations say their agency's security solutions are **collapsing** under growing SSL bandwidth demands and SSL key lengths

Learn how A10 Thunder SSLi delivers high-performance and cost-effective visibility into encrypted traffic, empowering your entire security infrastructure to defend your network against hidden threats.

Visit a10networks.com/ssli

Source:
Survey on Hidden Threats in Encrypted Traffic: Industry Verticals, Presented by Dr. Larry Ponemon. Ponemon Institute. March 27, 2016.

Part Number: A10-GR-70299-EN-01 July 2016